

Self-generating two-key system for data access protection

Publication number: DE3411570

Publication date: 1985-11-07

Inventor:

Applicant: KUEBLER MONIKA (DE)

Classification:

- international: **G06F21/00; G07F7/10; G06F21/00; G07F7/10; (IPC1-7): G06F12/14; G06F3/08; G06F7/58; G07F7/08**

- european: **G06F21/00N5A2D; G07F7/10E**

Application number: DE19843411570 19840329

Priority number(s): DE19843411570 19840329

Report a data error here

Abstract of DE3411570

Access protection by automatically generating a "password" unknown to the respective user himself, by using a random-number generator (or similar) in the user computer. - Storage and provision of this password in divided form (two- or multi-key system) on at least two independent permanent memories, at least one of which must be portable. (The latter is always physically located with the user such as cheque card and cheque book). - When accessing a computer centre, the separately stored password information items are assembled again and checked for known. If known, a new password is generated in the user computer, supplied to the computer centre and again stored in separate form. - The password in each case only has validity for a single self-contained data session and is automatically renewed in each subsequent session if a computer centre is accessed in the latter. The generation, maintaining and renewing of the password in connection with a necessary user number in the above system represents a data access protection which can be called 100%. It is only such protection which, for example, enables external tape transactions or similar to be performed.

Data supplied from the **esp@cenet** database - Worldwide

①9 BUNDESREPUBLIK
DEUTSCHLAND



DEUTSCHES
PATENTAMT

⑫ **Offenlegungsschrift**
⑪ **DE 3411570 A1**

⑳ Aktenzeichen: P 34 11 570.6
㉑ Anmeldetag: 29. 3. 84
㉒ Offenlegungstag: 7. 11. 85

㉓ Int. Cl. 4:
G 06 F 12/14
G 06 F 7/58
G 06 F 3/08
G 07 F 7/08

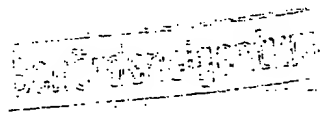
DE 3411570 A1

㉔ Anmelder:
Kübler, Monika, 7032 Sindelfingen, DE

㉕ Erfinder:
Antrag auf Nichtnennung

㉖ Recherchenergebnisse nach § 43 Abs. 1 PatG:

DE-OS 30 41 393
DE-OS 30 07 598
DE-OS 28 24 135
DE-OS 28 22 522
DE-OS 28 03 321
US 37 74 743
EP 00 89 876



Prüfungsantrag gem. § 44 PatG ist gestellt

㉗ Selbstgenerierendes Zweischlüsselsystem für Datenzugriffssicherung

Zugriffssicherung durch automatische Erstellung, eines dem jeweiligen Benutzer selber unbekannten 'Passwords' unter Verwendung eines Zufallgenerators (oder ähnlichem) im Benutzer-Computer.

- Speichern und Bereithaltung dieses Passwords in geteilter Form (Zwei- oder Mehrschlüsselsystem) auf mindestens zwei unabhängigen Permanentspeichern, wovon mindestens einer portable sein muß. (Jener befindet sich immer phys. beim Benutzer, wie Scheckheft und Scheckkarte.)

- Bei Zugriff zu einem Rechenzentrum werden die getrennt gespeicherten Password-Informationen wieder zusammengeführt und auf bekannt geprüft.

Wenn bekannt, wird im Benutzercomputer ein neues Password erstellt, dem Rechenzentrum mitgeteilt und erneut in getrennter Form abgespeichert.

- Das Password hat jeweils nur Gültigkeit für eine einzige abgeschlossene Datensitzung und wird bei jeder Folgesitzung automatisch erneuert, soweit in dieser ein Zugriff zu einem Rechenzentrum stattfindet.

Die Erstellung, Haltung und Erneuerung des Passwords in Verbindung mit einer notwendigen Benutzernummer in obigem System stellt eine als 100% zu bezeichnende Datenzugriffssicherung dar.

Erst eine solche Sicherung ermöglicht zum Beispiel externe Bandtransaktionen oder ähnliches.

DE 3411570 A1

Patentansprüche

1. Unter dem selbstgenerierenden Zweischlüsselsystem meine ich auch jede Art von Mehrschlüsselsystem, soweit dieses wie in der Hauptanmeldung näher beschrieben zum Einsatz kommt.
2. Die in der Hauptanmeldung näher beschriebene Benutzer-Nr. kann selbstverständlich auch direkt bei der Erstinitialisierung durch das Rechenzentrum auf der Magnetkarte (oä. portabler Speicher) gespeichert werden um somit eine manuelle Eingabe des späteren Benutzers und die damit verbundenen Fehlermöglichkeiten zu unterbinden.
3. Bei der in der Hauptanmeldung beschriebenen Magnetkarte handelt es sich nur um ein Beispiel eines portablen Speichers.
Jede Verwendung eines anderen portablen Speichers kann selbstverständlich auch Verwendung finden.
4. Der in der Hauptanmeldung beschriebene Zufallsgenerator kann selbstverständlich auch durch eine andere Funktion ersetzt werden, dessen Ergebniss letztlich jedoch ~~XXX~~ die in der Hauptanmeldung näher beschriebene 'Schlüsselerweiterung' darstellt.
5. Die Länge und Art der Schlüsselerweiterung ist ebenfalls frei, ob reiner 'Bitstring' oder nicht, ebenfalls die Aufteilung der Schlüsselerweiterung (Speicherung) auf den unabhängigen Speichern.
6. Ebenfalls der Zeitpunkt der Generierung einer Schlüsselerweiterung (ob bei Beginn einer Sitzung oder am Ende oder anderweitiger Zeitpunkt oder mehrfach in einer Sitzung oder irgendeine Art von Teilgenerierung) ist frei zu bestimmen.

M. Kübler



2.

Beschreibung : Selbstgenerierendes Zweischlüsselsystem für
Datenzugriffssicherung

Problemstellung(Aufgabe) :

Wie kann ein unberechtigter Datenzugriff in einem Rechenzentrum
(Fig. 2 (C)) sicher und praktikabel verhindert werden.
(Hecker Aktivitäten !!!)

oder

Wie kann das Rechenzentrum (C) Fig.2,eindeutig erkennen,ob
es sich bei einem jeweiligen Datenzugriff um einen zugelassenen
Benutzer (A) Fig. 2 handelt oder um eine unberechtigte
Simulation.

Lösung :

Bei der Idee handelt es sich um eine bis dato nicht angewendete
Verknüpfung,von in der Datenverarbeitungsbranche allgemein
bekannten Einzelfunktionen und Bauteilen zum Zwecke der
Datenzugriffssicherung.

Es gilt somit,nur die Idee zur Verknüpfung bestimmter Bauteile
und Funktionen zum Zwecke der Datenzugriffssicherung zu
schützen.

Folgende Bauteile und Funktionen werden bei der Idee verwendet:

1. Magnetkartenleser/Schreiber (o.ä.)

Da es hier die unterschiedlichsten Fabrikate auf dem
Markt gibt,möchte ich mich nur auf eine kurze Beschreibung
der Arbeitsweise eines solchen Bauteiles beschränken.
Dieses Bauteil ist in der Lage,Informationen auf einen
Datenträger(zB. Magnetkarte wie Scheckkarte)zu speichern
und zu lesen.

Der Datenträger kann dem Bauteil entnommen werden,wobei
die auf Ihm gespeicherten Daten erhalten bleiben.

Lösung :2. Magnetkarte(oä.portabler Speicher)

Hierbei handelt es sich um den in Punkt 1 angeführten Datenträger, Welcher mit einem Computer nicht fest verbunden ist.

Das heißt, Er kann dem Computer bei Bedarf zugeführt werden und befindet sich ansonsten direkt beim jeweiligen Computerbenutzer. (siehe Fig. 1 (A))

3. Permanent-Datenspeicher (Fig. 1 (G))

Im Gegensatz zur Magnetkarte oder einem portablen Speicher, ist Dieser fest im Computer eingebaut und kann von einem Benutzer nicht entfernt werden.

Ansonsten hat er die gleichen Grundeigenschaften wie eine Magnetkarte, Er kann Daten speichern und man kann (der Computer kann) Daten von Ihm lesen.

Auch bei Stromabschaltung bleiben die gespeicherten Daten erhalten.

4. Zufallsgenerator (Fig. 1 (F))

Hierbei handelt es sich um eine Funktion, Welche in der Lage ist, ein reines Zufallsergebniss in X-beliebiger Länge zu erzeugen. zB. "1gh4örosm440"

5. Benutzernummer (Fig. 1 (B))

Jeder Benutzer eines Rechenzentrums muss eine Benutzungsmöglichkeit vorher beim jeweiligen Rechenzentrum beantragen.

Wird diesem Antrag stattgegeben, so erhält der Antragsteller eine sogenannte Benutzernummer (ein Begriff, welcher im jeweiligen Rechenzentrum einmalig und dem Benutzer eindeutig zugeordnet ist.

Mittels dieser Benutzernummer kann der Benutzer sich nun, zB mit seinem 'Home Computer' datenmäßigen Zutritt zum Rechenzentrum verschaffen.

Zum Schutze der eigentlichen Daten wird in der Regel noch ein sogenanntes 'Password' angehängt, welches der Benutzer selber vergeben bzw. definieren kann.

Dieses 'Password' und dessen Erstellung ist der Schwachpunkt in der momentan weltweit betriebenen Datenzugriffssicherung und wird deshalb durch die folgend näher beschriebene Lösung voll ersetzt.

Lösung :

- Benutzernummer (FIG. 1 (B)) wird weiterhin vom Rechenzentrum vergeben
- Password wird nicht mehr vom Benutzer vergeben, sondern von einem Zufallsgenerator (Fig. 1 (F)). Das vom Zufallsgenerator ermittelte Password wird auf zwei oder mehrere unabhängige Speichermedien verteilt gespeichert.
zB. Magnetkarte (Fig. 1 (A))
+ Permanentpeicher (Fig. 1 (G))
Mindestens einer dieser Speicher muss portable sein, der Rest muss fest im Computer installiert sein.
Unter portable ist zu verstehen, das dieser Speicher vergleichbar mit einer Scheckkarte am Körper des Benutzers getragen werden kann.
Die nun getrennt gespeicherte Password-Information wird bei einem Datenzugriff auf ein Rechenzentrum automatisch von dem jeweiligen '#Home Computer' zusammengeführt und ersetzt die bisherige manuelle Password-Eingabe durch den Benutzer.
- Der Gesamt-Zugriffsschlüssel bestehend aus Informationen der Benutzernummer (Fig.1 (B))
+ Magnetkarte (Fig.1 (A))
+ Permanentpeicher (Fig.1 (G))
wird dem Rechenzentrum bei Beginn einer 'Datensitzung' automatisch mitgeteilt nachdem der alte, letzte oder ursprünglichste Stand mit dem gleichen Stand im Rechenzentrum verglichen wurde.
Bei fehlerhaftem Password (Zugriffsschlüssel) wird vom Rechenzentrum, mit einer gewissen Zeitverzögerung die Leitungsverbindung unterbrochen (Leitung muss neu angewählt werden).
Bei jeder einzelnen Datensitzung wird vom Home Computer ein neues Password erstellt, getrennt gespeichert und dem Rechenzentrum mitgeteilt (Fig. 1 (D))

- Sicherheit :

Durch die getrennte Haltung der Passwordinformationen
welche noch in unregelmäßigen Abständen automatisch
erneuert werden

plus

der unabhängigen Benutzernummer

plus

automatischer Auflösung der Leitungsverbindung verbunden
mit einer Zeitverzögerung vor neuer Anwählmöglichkeit

dürfte die Sicherheit als 100 % angesehen werden.

- Anwendungsmöglichkeiten :

Dezentrale Abwicklung von Bankgeschäften

Zugriffssicherung im BTX der Bundespost

Private dezentrale Datenverarbeitung

usw

Diese Möglichkeiten bestehen auf Grund fehlender oder
mangelhaften Zugriffssicherungen bis dato nicht
bzw. sind solche Anwendungen aus Sicherheitstechnischen
Gründen nicht zu empfehlen.

Gesamtablauf-Beispiel :Selbstgenerierendes Zweischlüsselsystem
für Datenzugriffssicherung

1. Der Benutzer beschafft sich einen Computer,unter anderem für Anwendungen auf einem Rechenzentrum.
2. Benutzer beantragt Zulassung zu einem Rechenzentrum.
3. Im Rechenzentrum läuft nun folgendes ab :
 - Anlegen einer im Rechenzentrum eindeutig dem Benutzer zugeordneten Benutzernummer,welche den späteren Einstiegsschlüssel ins Rechenzentrum darstellt.
 - Für den Benutzer wird entsprechend seines Antrages ein entsprechender Platz im Rechenzentrum bereitgestellt.
 - Für den Benutzer wird ein portabler Speicher (zB. Magnetkarte oder anderer Datenträger erst-initialisiert)
das heißt,um dem Benutzer einen ersten Zugriff auf ein Rechenzentrum zu ermöglichen muss ein sogenanntes 'Erstpassword' vom rechenzentrum erstellt werden, welches beim Erstzugriff im Rechenzentrum dann bekannt ist.
Beim Erstzugriff des Benutzers wird dann das eigentliche Password vom Benutzer-Computer automatisch neu erstellt und dem Rechenzentrum mitgeteilt nach vorheriger Überprüfung des 'Erstpasswords'.
Erst ab diesem Zeitpunkt hat der Benutzer richtigen Zugriff zum Rechenzentrum und auf die für Ihn dort vorgesehenen Programme oder Daten.
 - Jedes Neue incl. des 'Erstpasswords' wird im Rechenzentrum auf zwei phys.unabhängigen Speichern abgespeichert.
dieses ist notwendig für ein sogenanntes 'reload' (Zurückladen) der Daten bei Zerstörung der Datenträger oder ähnlichen Problemen.

- Der erstinitialisierte portable Speicher (zB. Magnetkarte) wird dem Benutzer in Verbindung mit seiner Benutzernummer vom Rechenzentrum übergeben.
4. Der Benutzer möchte nun die Arbeit mit dem Rechenzentrum beginnen :
- Der Benutzer steckt seine Magnetkarte oä. in seinen Computer
 - Stellt über Postleitung oder ähnliches die Verbindung zu Rechenzentrum her.
 - Gibt seine Benutzernummer manuell in seinen Computer ein, soweit diese nicht schon Bestandteil der Magnetkarteninformation ist.
5. Im Computer des Benutzers läuft nun folgendes ab :
- Die Benutzernummer wird um die Information der Magnetkarte (Fig.1 (A)) und der Information des permanent Speichers (Fig.1 (G)) erweitert. Der so entstandene Gesamtbegriff wird nun im Rechenzentrum auf bekannt geprüft. Bei Erstzugriff wird in diesem Fall die Benutzer-nummer nur um die Information der Magnetkarte erweitert.
 - Wenn Gesamtbegriff im Rechenzentrum unbekannt, wird die Leitungsverbindung nach einer Zeitverzögerung vom Rechenzentrum unterbrochen. (Muss neu angewählt werden)
 - Wenn der Gesamtbegriff im Rechenzentrum bekannt ist, erhält der Benutzer-Computer vom Rechenzentrum ein Signal, welches den Zufallsgenerator im Benutzer-Computer veranlaßt, ein neues Password zu erstellen, auf Magnetkarte und permanent Speicher in aufgeteilter Form zu speichern, es dem Rechenzentrum mitzuteilen.
 - Der nun folgende Informationsaustausch zwischen Rechenzentrum und Benutzer erfolgt nun über dieses neue Password in Verbindung mit der Benutzernummer. (und zwar nur für diese eine Sitzung)

9.

34 11 570

Fig. 1

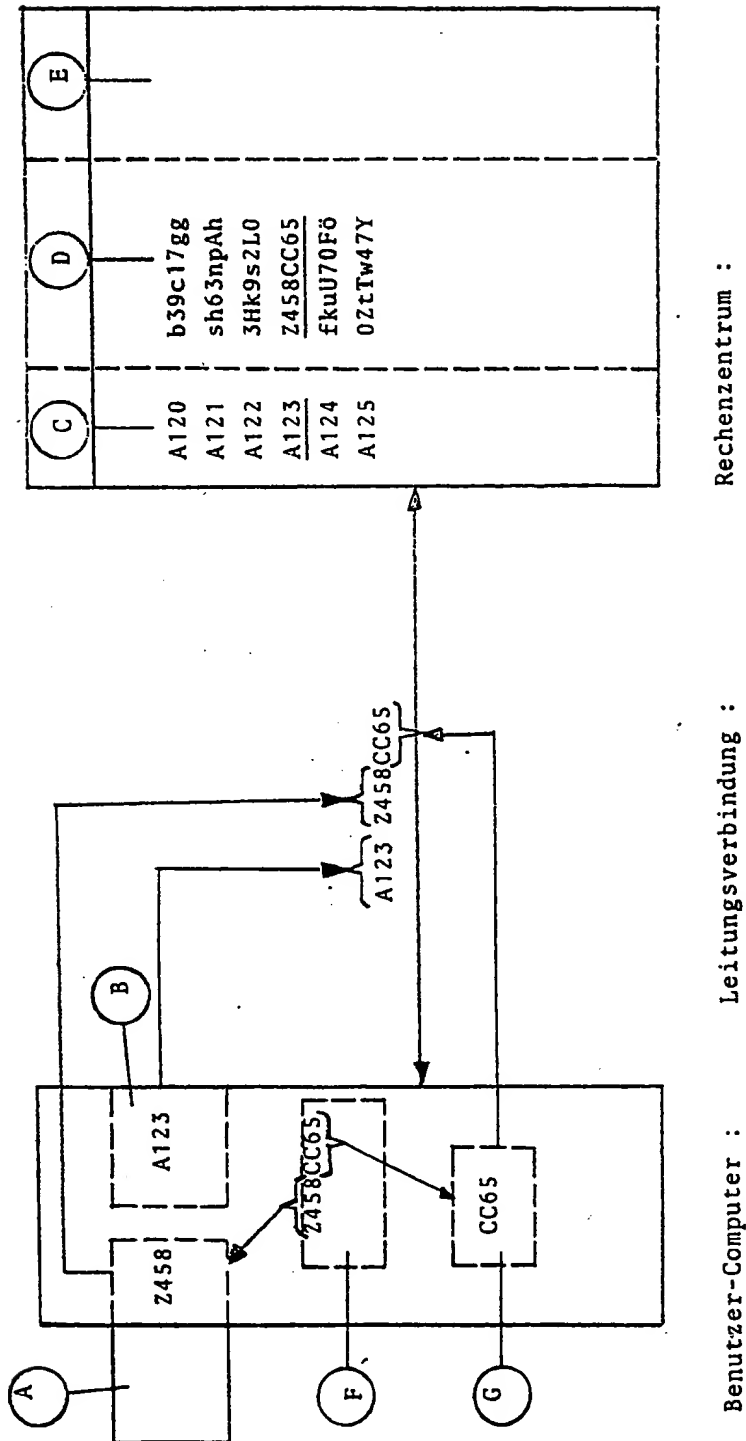


Fig. 2

